CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method of generating successive round keys of an expanded key from an initial cryptographic key for use in an encryption and/or decryption engine, comprising ~~the steps of~~:

storing ~~the~~ N_k words of the initial key in N_k locations of a memory;

providing the initial key to a cryptographic engine for performing a first cryptographic round;

repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory~~, and~~;

generating from the selected first and second words ~~a~~ successive subsequent ~~word~~ words of the expanded key;

providing the generated words of the expanded key to the cryptographic engine as round keys for performing subsequent cryptographic rounds; ~~and~~

storing successive ones of the generated ~~subsequent~~ words in the memory by cyclically overwriting previously generated words of the expanded key; and

maintaining four successive words from the generated words in the memory as long as they are required for use in the generation of subsequent words and for

use in a parallel operation of a cryptographic process, wherein the four successive words comprise a new round key.

2. (Currently Amended) The method of claim 1,

in which ~~the step of~~ overwriting said previously generated words only occurs after ~~those~~ said previously generated words have been used as said first and/or said second selected words ~~in the step of~~ while generating ~~a respective~~ said subsequent ~~word~~ words.

3. (Currently Amended) The method of claim 1,

in which ~~the~~ a number of memory locations used is less than ~~the~~ a number of words in the expanded key.

4. (Currently Amended) The method of claim 1,

in which ~~the~~ a number of memory locations used is equal to N_k.

5. (Currently Amended) The method of claim 4,

in which ~~the~~ words of the initial key are also overwritten by words of the expanded key during the overwriting ~~step~~.

6. (Currently Amended) The method of claim 1,

in which ~~the~~ a number of memory locations used is equal to $2N_k$.

7. (Currently Amended) The method of claim 1,

in which the memory is divided into two parts, a first part storing the initial key and ~~the~~ a second part receiving the successive ~~successively generated~~ words of the expanded key.

8. (Currently Amended) The method of claim 7, further including~~the step of~~:

completing generation of the expanded key such that ~~the~~ a final round key is stored in the second part of the memory and the initial key is still stored in the first part of the memory.

9. (Currently Amended) The method of claim 8, further including~~the step of~~:

performing a repeat key expansion starting with the initial key stored in the first part of the memory.

10. (Currently Amended) The method of claim 8, further including~~the step of~~:

performing an inverse key expansion starting with the final round key stored in the second part of the memory.

11. (Currently Amended) The method of ~~any one of claims 1~~ claim 1, further including ~~the step of~~:

completing generation of the expanded key such that ~~the~~ a final round key is stored in the memory and the initial key has been overwritten.

12. (Currently Amended) The method of claim 11, further including ~~the step of~~:

performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation.

13. (Currently Amended) The method of claim 7,

in which ~~the~~ a number of memory locations used is equal to $2N_k$, the first and the second parts having N_k locations each.

14. (Currently Amended) The method of ~~any preceding~~ claim 1, further comprising:

~~in which the step of generating successive subsequent words of the expanded key comprises~~:

generating successive words of ~~the~~ AES Rijndael block cipher round keys according to ~~the~~ an AES key expansion function.

15. (Currently Amended) The method of claim 14,

in which N_k=8.

16. (Currently Amended) The method of claim 1,

in which the successive subsequent words of the expanded key comprise words of encryption round keys.

17. (Currently Amended) The method of claim 1,

in which the successive subsequent words of the expanded key comprise words of decryption round keys.

18. (Currently Amended) The method of claim 1, further comprising:

~~in which the step of providing the generated words of the expanded key to the cryptographic engine comprises~~

providing the generated words on a word-by-word basis as the cryptographic engine consumes the generated words as round keys.

19. (Currently Amended) The method of claim 1,

in which~~, in the retrieving step,~~ both the selected first word and the selected second word are retrieved from the memory.

20. (Currently Amended) The method of claim 1,

in which~~, in the retrieving step,~~ the selected first word is retrieved from memory and the selected second word is retrieved from a register used in a previous iteration.

21. (Currently Amended) The method of claim 1,

in which ~~the step of~~ providing the generated words of the expanded key to the cryptographic engine comprises:

providing said generated words from the memory.

22. (Currently Amended) The method of claim 1,

in which ~~the step of~~ generating includes, in at least some cycles of round key word generation, ~~the step of~~ performing an S-box transform using an S-box shared with the cryptographic engine.

23. (Currently Amended) The method of claim 22, further comprising

~~including the step of:~~

maintaining synchronism of the generation of successive round key words with consumption of the round key words by the cryptographic engine.

24. (Currently Amended) A round key generator for generating successive round keys of an expanded key from an initial cryptographic key for use in an encryption and/~~or~~ decryption engine, comprising:

a memory for storing ~~the~~ N_k words of the initial key;

an expansion processor for

repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory, and

generating from the selected first and second words ~~a~~ successive subsequent ~~word~~ words of the expanded key;

means for providing the generated words of the expanded key to the ~~cryptographic~~ encryption and decryption engine as round keys for performing subsequent cryptographic rounds;

means for storing the successive ~~ones of the generated~~ subsequent words in the memory by cyclically overwriting previously generated words of the expanded key; and

means for maintaining four successive words from the generated words in memory as long as they are required for use in the generation of subsequent words and for use in a parallel operation of a cryptographic process, wherein the four successive words comprise a new round key.

25. (Currently Amended) The apparatus of claim 24, further including:

control means for ensuring said previously generated words are overwritten only after ~~those~~ said previously generated words have been used as said first and/or said second selected words by the expansion processor.

26. (Currently Amended) The apparatus of claim 24,

in which ~~the~~ a number of word locations in memory is less than ~~the~~ a number of words in the expanded key.

27. (Currently Amended) The apparatus of claim 24,

in which ~~the~~ a number of word locations in the memory is equal to N_k.

28. (Currently Amended) The apparatus of claim 27,

in which ~~the~~ words of the initial key are also overwritten by words of the expanded key during the overwriting.

29. (Currently Amended) The apparatus of claim 24,

in which ~~the~~ a number of word locations in the memory is equal to $2N_k$.

30. (Currently Amended) The apparatus of claim 24,

in which the memory is divided into two parts~~,~~:

a first part storing the initial key, and

~~the~~ a second part receiving the successively generated words of the expanded key.

31. (Currently Amended) The apparatus of claim 30,

in which the means for storing stores ~~the~~ a final round key in the second part of the memory and retains the initial key in the first part of the memory after completion of generation of the expanded key.

32. (Currently Amended) The apparatus of claim 31, further including:

means for performing a repeat key expansion starting with the initial key stored in the first part of the memory.

33. (Currently Amended) The apparatus of claim 31, further including:

means for performing an inverse key expansion starting with the final round key stored in the second part of the memory.

34. (Currently Amended) The apparatus of ~~any one of~~ claim 24, further including:

means for completing generation of the expanded key such that ~~the~~ a final round key is stored in the memory and the initial key has been overwritten.

35. (Currently Amended) The apparatus of claim 34, further including:

means for performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation.

36. (Currently Amended) The apparatus of claim 30,

in which ~~the~~ a number of word locations in the memory is equal to $2N_k$, the first and the second parts having N_k locations each.

37. (Currently Amended) The apparatus of ~~any preceding~~ claim 24,

in which the expansion processor includes means for generating successive words of ~~the~~ AES Rijndael block cipher round keys according to ~~the~~ an AES key expansion function.

38. (Currently Amended) The apparatus of claim 37,

in which N_k=8.

39. (Currently Amended) The apparatus of claim 24,

in which the expansion processor generates words of encryption round keys.

40. (Currently Amended) The apparatus of claim 24,

in which ~~the~~ an expansion key processor generates words of decryption round keys.

41. (Currently Amended) The apparatus of claim 24, further including:

a cryptographic engine, and

means for providing the generated words of the expanded key to the cryptographic engine on a word-by-word basis as the cryptographic engine consumes the words as round keys.

42. (Currently Amended) The apparatus of claim 24, further including:

means for retrieving both the selected first word and the selected second word from the memory.

43. (Currently Amended) The apparatus of claim 24, further including:

means for retrieving the selected first word from the memory and the selected second word from a register in the expansion processor.

44. (Currently Amended) The apparatus of claim ~~1~~ 24, further including:

a cryptographic engine, in which the expansion processor and the cryptographic engine share an S-box.

45. (Currently Amended) The apparatus of claim 44, further including:

~~the~~ means for maintaining synchronism of the expansion processor and the cryptographic engine.

46. (Currently Amended) ~~A smart card incorporating the~~ The round key generator ~~according to~~ of claim 24, further comprising:

a smart card.

47. (Canceled).

48 (Currently Amended) The method of claim ~~47~~ 1,

in which the initial key ~~words are also~~ is maintained in the memory ~~during the entire process of~~ while generating successive subsequent words of the expanded key.

49-54. (Canceled).